Module- 2

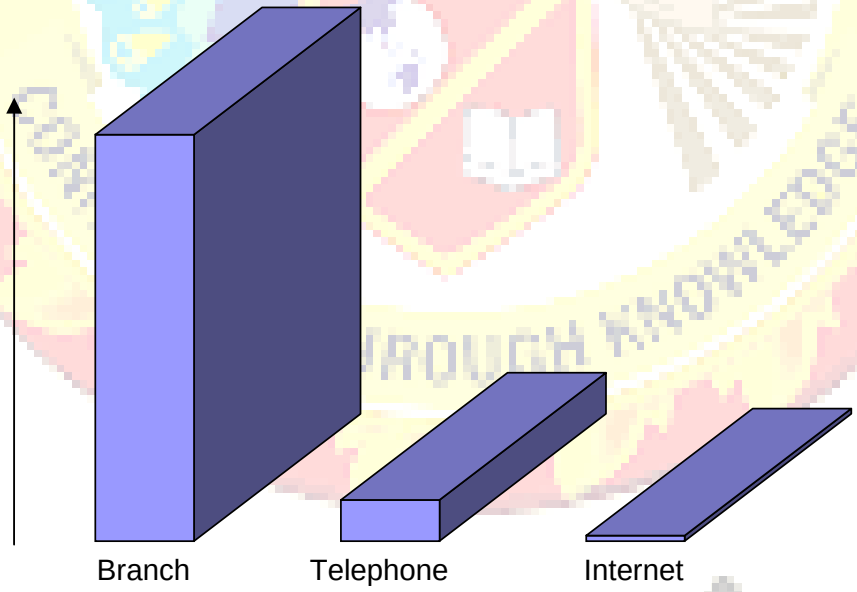
Authentication Management

Introduction

The Internet is the fastest growing banking channel today, both in the fields of corporate and retail banking. The development is no longer just driven by the banks' desire to reduce costs: first and foremost, it is a manifestation of customers' demand to access bank services on-line—at any time and from any location.

The importance of Internet banking is obvious for several reasons. Firstly, it offers a cost-efficient alternative to telephone and branch banking due to the relatively low capital and maintenance costs, and its fully automated processing of most transactions. Secondly, it offers unparalleled customer convenience by enabling 24-hour access to a wide range of services.

The cost of different banking channels



Despite this win-win proposition, Internet banking is not without its drawbacks. Foremost among these in recent years has been the widespread targeting of on-line banking systems by international criminal gangs, by means of a variety of attacks.

1 Threats and Countermeasures

1.1 Attacks on Internet Banking

The first 'phishing' emails targeting on-line financial systems were seen in 2001, as a 'Post 911 ID check' following the September 11 attacks on the World Trade Centre[1]. From 2004 onwards, the industry has seen a dramatic rise in attacks against both large and small financial institutions worldwide.

In parallel with this growth in attack volume, there has been a parallel rise in the variety and complexity of attacks. Banking security experts must now be familiar with a bewildering array of techniques and terminology: phishing, pharming, spear phishing, session hijack, man-in-the-middle, man-in-the-browser, Trojans, Rock Phish…the list goes on.

Despite the diversity in attack methods, most aim to achieve the same objective: to obtain confidential user information, such as usernames, passwords, credit card numbers and social security numbers. These are all *static* credentials—they don't change—and therein lies the problem. Once obtained, they can be used by the attacker to impersonate the customer to perpetrate fraud.

1.2 Two-Factor Authentication

Whilst it is useful to try to counter specific attacks (and as part of a layered security strategy, we would always recommend this), the only long-term, strategic solution is to move away from the current dependence on static credentials.

Traditionally, all authentication mechanisms can be placed into one of the following three categories:

- Something you **know**—a secret, such as a password.
- Something you **are**—a biometric, such as a fingerprint.
- Something you **have**—a device or object or some kind, such as a credit card.

With this approach, it can readily be seen that the problems with phishing arise from an over-reliance on the first category. Strong authentication can be achieved by employing two different authentication credentials in parallel, from *different* categories. This is known as *Two-Factor Authentication (2FA).*

For reasons of cost, complexity, reliability and privacy, biometrics are not widely used in banking. There are however a wide variety of low-cost, dependable security devices available.

Typically, such devices generate and display a *One-Time Password (or OTP).* As the name suggests, an OTP is valid for a single use only, and many are also time-limited. Rather than being static, OTPs are *dynamic*—new OTPs can be generated on demand, from an inexhaustible sequence that is unique to each device.

The OTP is copied from the device to the web terminal by the customer. To the bank, knowledge of a valid OTP demonstrates proof of possession of the device, which when coupled with a traditional static password can offer an extremely effective defence against on-line attacks.

1.3 Attacks Against 2FA

A small number of successful attacks against 2FA-enabled Internet banking systems have led to press reports that 2FA as a general approach has been ‘broken’. The reality is rather more complex, as we shall discuss below.

An attacker may obtain a valid OTP from a customer using the same methods as those used to obtain a static password. If the bank has deployed a simple system with 2FA used for log-in only, this attack may succeed.

To understand how to mitigate or eliminate this risk, it is first necessary to understand how attackers operate. Rather than one individual or organisation being responsible, attacks are carried out by loose associations of individuals or groups, each with their own specialist role. Different parties cooperate, each providing a service: creating a fake web site, sending spam email, collecting passwords, and finally using those passwords to obtain cash.

Passwords and other credentials are bought and sold between groups. This takes time. Since most OTPs include an expiry mechanism, the attacker’s standard operating model is no longer effective, and a considerably more complicated model of real-time attacks is being

adopted. This explains the continuing technological advances in on-line attacks which we discussed earlier.

Is this a never-ending arms race, or will there eventually be an outright winner? Happily, the strongest forms of 2FA available today offer a long-term, provably secure solution. The key is to move from authenticating the customer, to authenticating the transaction which the customer wishes to perform.

The user experience remains simple: the user simply enters the beneficiary account number and transaction amount into their authentication device, by means of an integral keyboard. The OTP thus created acts as a digital signature on those transaction details—even if obtained by an attacker, the OTP cannot be used for *any* other purpose.

Whilst this step may not be necessary today, many banks are deploying 2FA solutions with the option to upgrade to transaction authentication in the future. By this route, their customers first gain familiarity with the simplest form of the technology, and the bank is strategically placed to respond to future threats.

2 Deployment Options

2.1 Authentication Methods

Any bank considering deploying 2FA must choose between a wide range of possible authentication devices. The following list, whilst not exhaustive, gives a representative sample.

EMV Card and Reader

MasterCard has devised a scheme based on existing retail banking smart cards and PINs. Dubbed the Chip Authentication Program (CAP), it has also been adopted by Visa, under the Dynamic Passcode Authentication (DPA) banner.

The customer is supplied with a small, hand-held card reader, into which their existing EMV 'Chip and PIN' card is inserted. On entering the card PIN, the chip on the card is used to generate an OTP, which is displayed on the reader's screen. Additional functions on the reader also support transaction authentication.

The advantages include a high security, whilst by leveraging existing cards and issuance processes deployment and management costs are reduced. However, the user experience, whilst familiar, is more complicated than with other tokens.

Hardware & Software OTP Tokens

Many vendors offer OTP-generating tokens. They are available in a wide range of shapes and sizes, and many offer custom branding options.

The simplest tokens are suitable for user authentication only. More advanced tokens incorporate a keyboard, making them suitable for transaction authentication.

Most vendors employ proprietary algorithms to generate the OTPs. However, the Initiative for Open Authentication (OATH, see www.openauthentication.org) is an industry consortium promoting standardisation and interoperability.

Hardware-based PKI Tokens

A PKI system employs a *private key*, used to make *digital signatures* that are validated using a *public key*. The public key is held by the bank, and the private key by the customer.

Chip-card or USB devices are commonly used to secure the customer's private key. Since PKI tokens cannot generate OTPs, they must instead be connected to the customer's PC.

Devices and keys are often managed using a *Certificate Authority*.

They offer a high security level, although PC-based attacks may use the token illicitly. By including the ability to sign transactions and other instructions, they offer great flexibility to banking applications. As a result, they are more common in business banking than consumer banking.

Software-Based PKI Tokens

Rather than storing PKI private keys in a physical device, they can also be stored on the customer's PC, protected by software. By eliminating the device, such systems offer significant cost savings in distribution and maintenance.

However, the software-based signing key may be vulnerable to PC-based attacks, and since the key is installed on a particular PC, customer mobility is reduced.

SMS-based OTPs

An appealing alternative to deploying tokens is to use something the customer already has—their mobile phone. In this case, the bank generates the OTP and sends it to the customer as an SMS message. The customer returns the OTP to the bank through their web browser.

Naturally, this approach relies on the bank maintaining current details of the customer's telephone number and the customer being able to receive messages at the particular moment of logon.

Additionally, a transaction summary may be included in the SMS. This enables the user to detect fraudulently modified transactions.

01	492380	11	803432
02	952334	12	342039
03	102875	13	689452
04	028942	14	439773
05	680328	15	569034
06	240935	16	184943
07	023941	17	439023
08	678304	18	649357
09	802439	19	093494
10	225894	20	748399

TAN Lists

TAN (Transaction Authentication Number) lists are paper-based lists of one-time passwords. They are securely generated by the bank and issued to each customer.

The customer provides an OTP every time she logs on or submits a transaction. The OTPs are either used in sequence, or the bank requests a specific OTP using an index.

Whilst offering a lower security level, this low-technology approach offers a combination of simplicity, reliability and low cost.

Matrix Cards

Also called grid card, this is a random grid of numbers or letters typically printed on a credit-card sized piece of plastic issued by the bank.

The customer is prompted to supply the contents of 2 or 3 cells during logon or when submitting a transaction. For example, the prompt “A4, C7” would give the log-on response “5, 8” using the card shown.

With similar advantages to TAN lists, the card format is convenient and durable. Whilst re-use of cells make the security analysis less clear, it also allows for a more flexible expiry policy.

2.2 Pros and Cons

To compare authentication methods, they must each be assessed against a range of criteria:

- **Customer acceptability**—ease of deployment and use, portability and reliability
- **Cost**—initial purchase, deployment, support, lifetime and replacement
- **Effectiveness**—how effective is it against a wide range of simple and advanced attack scenarios?

Table 1 below gives a simple comparison of the main features of the authentication methods discussed previously.

Advantages	Method	Disadvantages
Simple to use Timely authentication	Hardware OTP tokens	User authentication only on simple models Cost of tokens
Simple to use Many users already carry capable smart phones Timely authentication Low cost	Software OTP tokens	User authentication only on simple applications Applications can be compromised
Transaction & user authentication Card PIN provides 2nd factor—no need for separate password Simple deployment	CAP/DPA	Cost of card readers Possible card reissuing costs Usability for some customers
Small form-factor Low cost Easy to use	Matrix card / TAN list	User authentication only Lower security level Easy to copy Relatively short lifetime
Transaction & user authentication Timely authentication Low initial cost Most users already carry mobile phones	SMS	Customer management expensive Availability to all customers Availability of coverage Ongoing cost of SMS messages
Transaction & user authentication Highly secure digital signature	PKI token (hardware / software)	Low user mobility Vulnerable to PC Trojans Hardware costs (high) High integration and support costs Internet channel only
Useful as second factor Familiar to all customers	Static & partial password / PIN	Very low security if sole method Password reset/PIN mailer costs

Table 1: Comparison of authentication methods